CYBSEC S.A.
Security Systems

"El Estado del Arte de la Seguridad Informática"

Lic. Julio C. Ardita
jardita@cybsec.com

Septiembre de 2005
Buenos Aires - ARGENTINA

Soluciones de Seguridad Informática
Sirviendo a Latinoamérica y Caribe

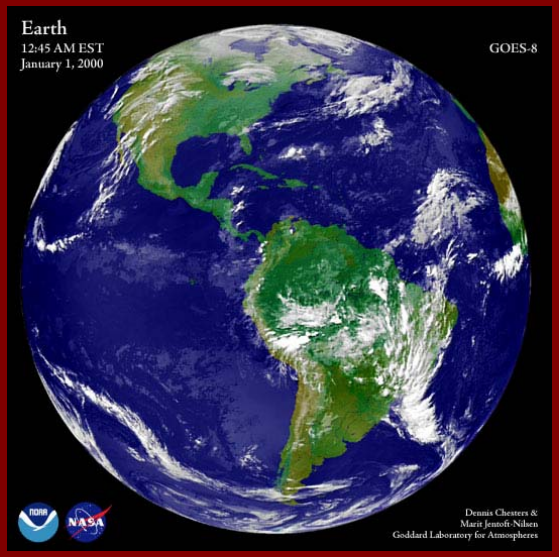
Agenda

- Problemática de la seguridad informática
- Situación en nuestro país
- Tendencias de las Tecnologías en Seguridad Informática

Problemática de la Seguridad Informática

Realidad

- Los mismos desafíos
- Mayores responsabilidades
- Pocos recursos
- Nivel de maduración
- Regulaciones



Realidad

CYBSEC descubrió 6 vulnerabilidades durante el presente año.

Vulnerabilities reported

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2005

Year	2000	2001	2002	2003	2004	1Q-2Q,2005
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	2,874

Total vulnerabilities reported (1995-2Q,2005): **19,600**

© CERT/CC

*La seguridad informática hoy**

El mercado aparentemente no reacciona ante los problemas de seguridad informática, vulnerabilidades básicas siguen apareciendo en los programas, los administradores todavía no realizan upgrades y no aplican patches a los sistemas y los usuarios siguen haciendo click sobre los archivos adjuntos enviados por correo electrónico.

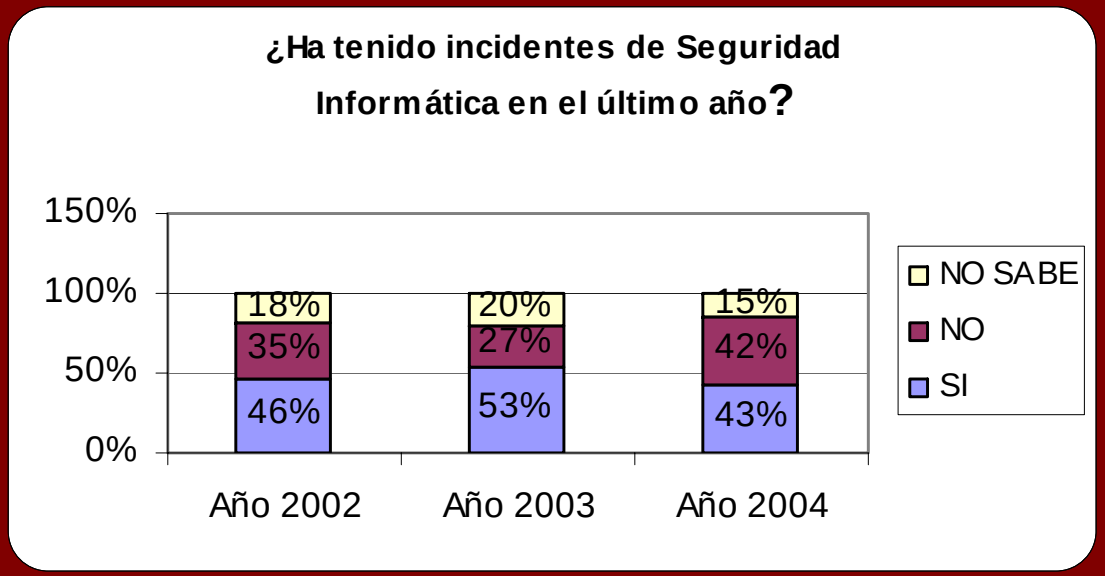
*La seguridad informática hoy**

Las empresas no pueden solucionar los problemas de seguridad porque si lo hacen, las aplicaciones críticas que están en producción entran en crisis y los proveedores siguen tratando de explicar que tener permisos habilitados para todo el mundo, utilizar usuarios genéricos y guardar passwords en plano, no es tan inseguro.

* Transparencias año 2002.

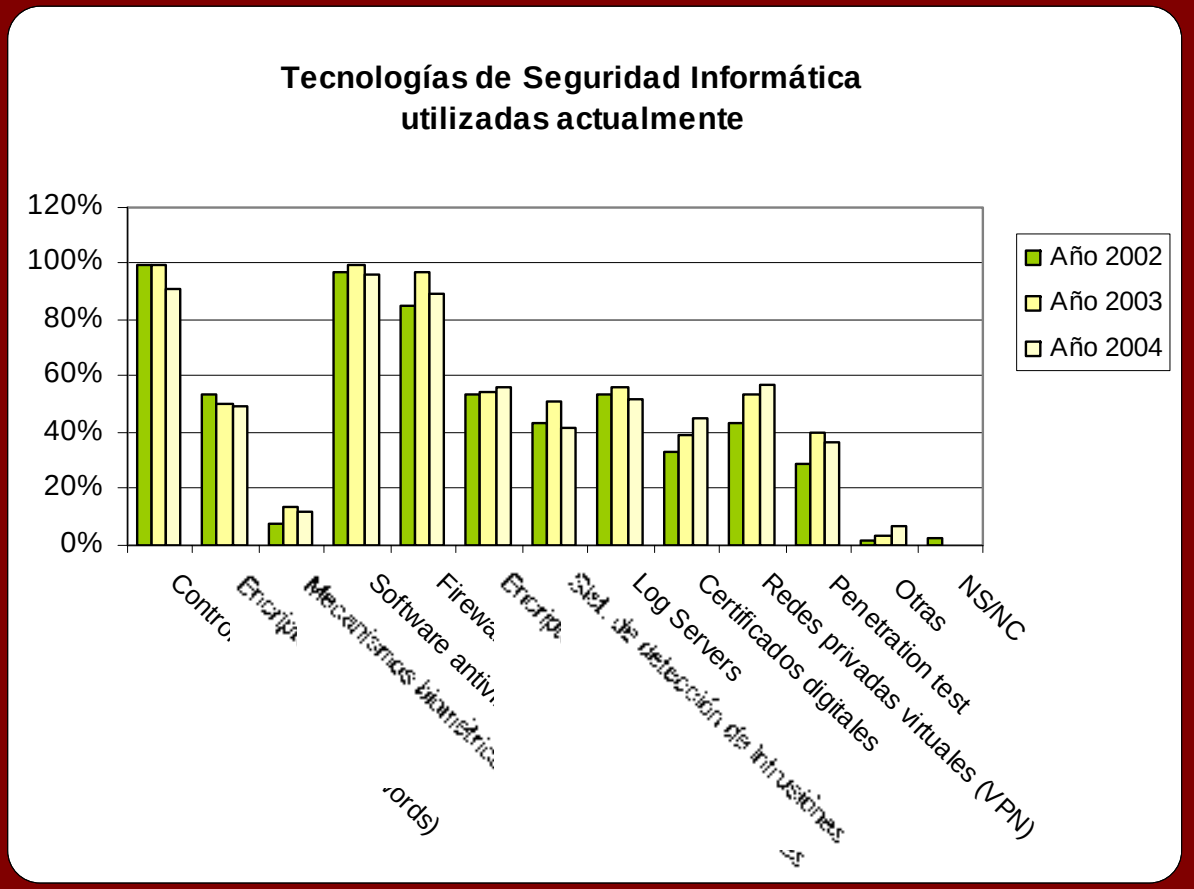
Situación en nuestro país

El 43% de las empresas manifestó haber tenido incidentes de seguridad informática en el último año. De éstas el 58% citó como primera fuente de ataque a Internet.



El Estado del Arte de la Seguridad Informática

Situación en nuestro país



El Estado del Arte de la Seguridad Informática

Situación en nuestro país

CYBSEC S.A. Security Systems

Los ataques más comunes durante el último año fueron los virus informáticos, el spamming de correo electrónico y el abuso del acceso a Internet.

Durante el año 2005 las empresas planean implementar tecnologías de sistemas de detección de intrusiones, penetration tests, redes privadas virtuales (vpn) y certificados digitales.

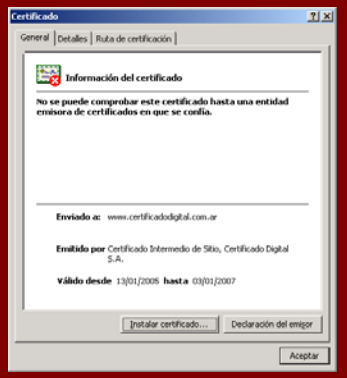
El 63% de las Organizaciones planea incrementar la inversión en Seguridad Informática.

Tendencias de las Tecnologías en Seguridad Informática

Tecnologías aceptadas

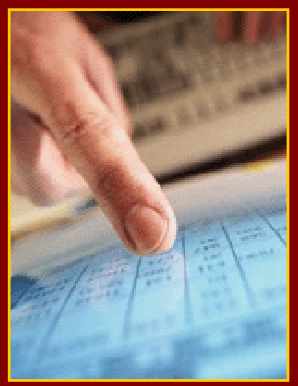
Existe un conjunto de tecnologías de seguridad informática que ya son comúnmente aceptadas:

- Políticas y normas de seguridad informática.
- Firewalls – Correcta implementación y actualización.
- VPN – Aspectos de seguridad en el Concentrador y Clientes.
- Encriptación.
- Anti-virus – Política y actualización.
- Certificados digitales – Servidores.



Management de la Seguridad Informática

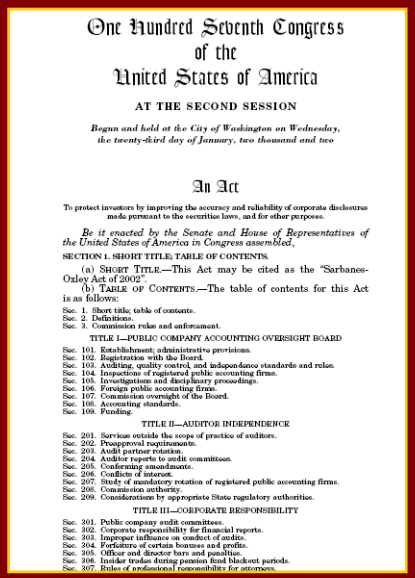
- Integración de la Seguridad Informática en el proceso de negocios de la Organización – Participación.
- Elaboración e implementación de un Plan de Seguridad Informática para cumplimentar las Políticas definidas.
- Establecimiento de métricas para poder "medirnos".
- Imposición de medidas de seguridad a los proveedores.
- "Vender" correctamente la seguridad informática.



Normativas

Las Organizaciones se están encontrando con normativas que las afectan. Se deben considerar aliadas.

- Regulaciones del Banco Central, Superintendencias, etc.
- Sarbanes-Oxley.
- ISO 17799.



One Hundred Seventh Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Wednesday, the twenty-third day of January, two thousand and two

An Act

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Sarbanes-Oxley Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. Commission rules and enforcement.

TITLE I—PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

Sec. 101. Establishment; administrative provisions.
Sec. 102. Registration with the Board.
Sec. 103. Auditing, quality control, and independence standards and rules.
Sec. 104. Inspections of registered public accounting firms.
Sec. 105. Investigations and disciplinary proceedings.
Sec. 106. Foreign public accounting firms.
Sec. 107. Commission oversight of the Board.
Sec. 108. Accounting standards.
Sec. 109. Funding.

TITLE II—AUDITOR INDEPENDENCE

Sec. 201. Services outside the scope of practice of auditors.
Sec. 202. Preapproval requirements.
Sec. 203. Audit partner rotation.
Sec. 204. Auditor reports to audit committees.
Sec. 205. Conforming amendments.
Sec. 206. Conflicts of interest.
Sec. 207. Study of mandatory rotation of registered public accounting firms.
Sec. 208. Commission authority.
Sec. 209. Considerations by appropriate State regulatory authorities.

TITLE III—CORPORATE RESPONSIBILITY

Sec. 301. Public company audit committees.
Sec. 302. Corporate responsibility for financial reports.
Sec. 303. Improper influence on conduct of audits.
Sec. 304. Forfeiture of certain bonuses and profits.
Sec. 305. Officer and director bars and penalties.
Sec. 306. Insider trades during pension fund blackout periods.
Sec. 307. Rules of professional responsibility for attorneys.

Management de LOGS

Los **LOGS** ya son considerados **evidencia crítica**. No se puede alegar desconocimiento sobre configuración de los mismos.

- Definición de Política de LOGS (Qué, Cuanto, Como, Donde).
- Centralización de LOGS.
- Explotación de LOGS.
- Herramientas de correlación de eventos.

PKI

- Las organizaciones han desistido de utilizar grandes infraestructuras de PKI.

- Están utilizando solamente lo que necesitan: AC Internas.

- Usos:

  - Certificados digitales para Web Servers internos.
  - Certificados digitales en Clientes para autenticación.
  - Certificados digitales para VPN.

Concientización

Generar procesos de concientización en seguridad informática:

- **Nivel directivo (Artículos, eventos, demostración de riesgos).**
- **Nivel gerencial (Charlas, Informes, etc).**
- **Nivel usuario (Cursos, folletos, etc).**

Prevención de ataques de ingeniería social.

Proyectos informáticos en un entorno seguro

La tendencia es incorporar la seguridad informática desde el nacimiento del proyecto.

- Lineamientos de seguridad.
- Desarrollo de aplicaciones.
- Instalación y configuración.
- Prueba pre-producción.
- Mantenimiento y soporte técnico.

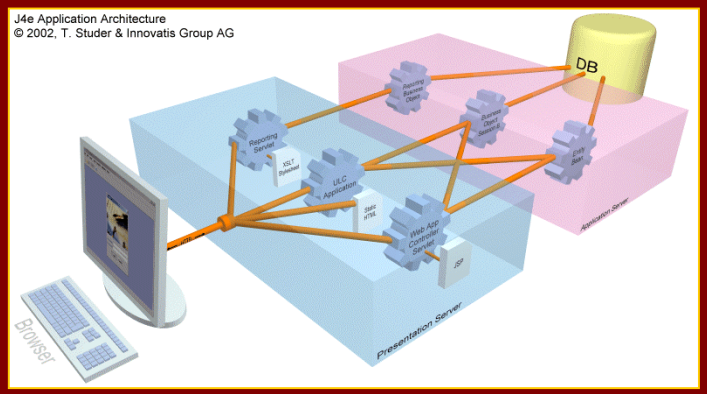
Seguridad en aplicaciones WEB

Las nuevas aplicaciones que se desarrollan son Web-enable. Esto permite a una organización desarrollar aplicaciones internas y que rápidamente puedan ser utilizadas en Extranet y/o Internet.

Programación segura de aplicaciones web (impedir buffer-overflow, cross-site scripting, path transversal y sql injection, entre otras).

- Medidas anti-phishing.

- Medidas anti-keyloggers.



Seguridad en redes inalámbricas

- Implementar aspectos de seguridad de la tecnología.
- No utilizar WEP Estático.
- Utilizar WPA/WPA2.
- La red Wireless debe ir a una DMZ.

Sistemas de Detección de Intrusiones (IDS)

- Maduración de la tecnología de IDS de red y de host.
- Utilización actual de NIDS en:
  - Monitoreo de DMZ´s.
  - Monitoreo de Internet.
  - Monitoreo de redes internas de Servidores.
- La tecnología de HIDS no se utiliza ampliamente, debido a:
  - Utilización de recursos en el Equipo.
  - Falta de diseño en la actualización y mantenimiento.
  - Costo.

Sistemas de Detección de Intrusiones (IDS)

Monitoreo de Internet:

El 80% de los ataques son intentos de conexiones Netbios (Worms/Virus) y el 18% son herramientas automatizadas de scanning.

Monitoreo de DMZ´s:

- Ataques de scanners automatizados.
- Sólo un porcentaje muy ínfimo es un ataque real y es necesario investigar.
- Análisis de nuevos exploits.

Problemática del Operador.

Sistemas de Prevención de Intrusiones (IPS)

Los IPS actualmente se utilizan en los enlaces WAN para frenar los worms internos o en la conexión con Internet.

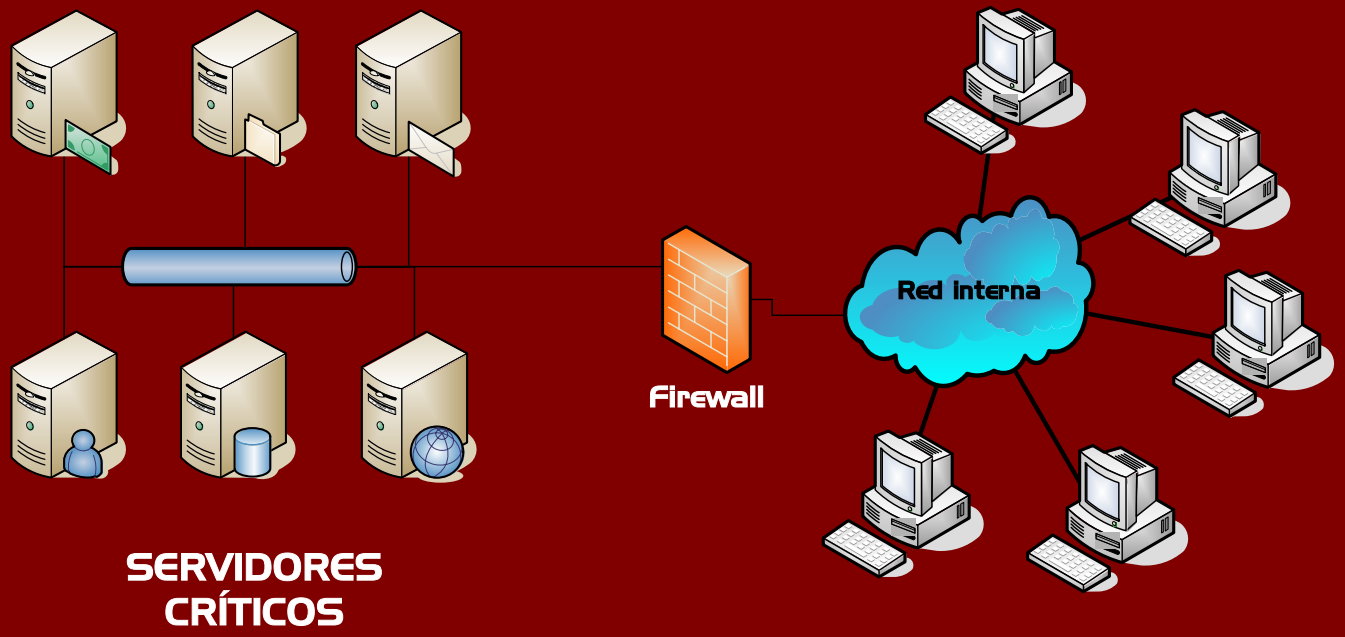
Depende la ubicación, necesitan un tunning muy avanzado para ser altamente efectivos.

Se basan en los IDS, pero bloquean el tráfico considerado intrusivo.

Requiere de un Administrador con conocimientos avanzados.

Protección de Servidores críticos

Existe la tendencia a Proteger los Servidores críticos de la propia red interna. Se utilizan Firewalls, IDS/IPS.



Penetration Test

- Incorporar al Penetration Test en el proceso de la Seguridad Informática.
- Nivel de madurez elevado en el mercado.
- Diferentes fines: conocimiento, validación de proyectos, un "seguro".
- Clave del Penetration Test: Definición del alcance.
- Aumento constante de la complejidad del PT.
- Aplicación de medidas correctivas.

Seguridad en sistemas propios

- Los sistemas propios son aquellos que procesan transacciones comerciales.
- Regulaciones de las Administradoras de Tarjetas de Crédito en relación a la seguridad.
- Estándares de seguridad para la operación con tarjetas.
- Adecuación de las Organizaciones.

Análisis Forense Informático

El servicio de análisis forense informático crece a un ritmo acelerado, debido a que muchos fraudes son cometidos utilizando medios tecnológicos.

Las organizaciones ya están desarrollando normativas y lineamientos a seguir en casos de incidentes de seguridad informática.

Mantenimiento de la seguridad

- La seguridad informática es **DINÁMICA** y por eso requiere indefectiblemente de un mantenimiento permanente.

- Establecimiento de una Política de Mantenimiento de la Seguridad en los sistemas informáticos (Dispositivos, Servidores, Estaciones de Trabajo y Aplicaciones), que incluya:

  - Corrección de Vulnerabilidades.
  - Aplicación de Patches de Seguridad.
  - Monitoreo de LOGS.

Educación

- Información masiva sobre seguridad informática en todos los niveles.
- Sites de referencia (Securityfocus, PacketStorm, etc).
- Oferta de educación en todos los niveles en seguridad informática.
- Formación de recursos humanos capacitados.

Conclusiones

- Para ser efectiva, la seguridad informática debe integrarse en los procesos de negocio de una Organización.

- Es muy importante considerar el factor humano y dedicarse a la concientización de los mismos.

- Hoy en día existen tecnologías y herramientas que van adquiriendo un mayor grado de maduración y nos permiten poder implementar y mantener sistemas informáticos seguros.

Preguntas?